REMARKS

Claims 1 – 6 are pending in this application. Claims 1, 2, 4, and 5 have been amended.

In a Non-Final Office Action mailed 19 May 2008, the Examiner rejected claims 1 – 6 under 35 USC 103(a) as being unpatentable over Gammie (U.S. Patent No. 5,237,610, hereinafter "the Gammie Patent), in view of Bilbrey (U.S. Patent Application Publication No. 2002/0164156, hereinafter "the Bilbrey Publication"), noting with respect thereto:

> Gammie discloses a wireless interface for Removable Digital Content Security Devices for delivering a stream of decrypted program content to a plurality of consumer electronics devices, comprising:
>
> security device means, removably connected to a first consumer electronics device, for receiving a stream of encrypted program content from a source [figure 5, decoder 506 receives encrypted program content through satellite link 505; output 509 will be inherently removably (as the user can disconnect the satellite receiver/decoder at any given time) connected to a TV, VCR, etc.];
>
> decryption means, located in said security device means, for converting said received encrypted program content to decrypted program content [column 6, lines 26-30, program descrambler 508 reads the decrypted key and uses the key to descramble and {sic} output descrambled program]; 508 is located within decoder 506];
>
> Gammie does not disclose authentication means, located in said security device means, for discovering the presence of at least one other consumer electronic device not connected to said security device means or said first consumer device, a link management means for establishing a wireless communication link from said security device means to said located at least one other consumer electronic device, or a wireless transmitter means for wirelessly transmitting said decrypted program content to at least one other consumer electronics device. Bilbrey discloses a portable video playback device adapted to receive compressed video data via an antenna and RF receiver [paragraph 34; it is inherent that an RF transmitter is paired with an RF receiver]. Bilbrey does not disclose discovering the presence of at least one other consumer electronics device or establishing the wireless communication link. 802.11 protocols were well known in the art at the time of invention (specifically 802.11a and 802.11b). As is known in the art, 802.11 wireless routers broadcast their SSID's and wireless enabled user devices discover the wireless networks and if a user decides to connect to the router via wireless enabled user device, the router and wireless enabled user device set up a communication link. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method and system for wirelessly transmitting and receiving

> digital content disclosed by Bilbrey with the well known methods of the 802.11 protocols in order to provide over-the-air modulation techniques using a basic protocol. Additionally, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system and method of Gammie with the wireless transmitting and receiving of Bilbrey and the 802.11 protocol in order to reproduce compressed video information by a portable device [paragraph 4].

Applicants have reviewed the cited references and the Examiner's stated grounds for rejection, and present the following arguments in support of patentability of Applicants' amended claims. In particular, the confusing "at least one" language and the lack of "automatically" limitations in the independent claims have been corrected so that the independent claims conform to Applicants' arguments.

In particular, Applicants' Removable Digital Content Security Device is removably installed in a first consumer electronics device and receives coded program content that is transmitted by a program source. The Removable Digital Content Security Device decodes the received content for use by the consumer in the first consumer electronics device. Applicants' Removable Digital Content Security Device also includes a wireless interface which serves to deliver the decoded program content to a second (or a plurality of) television or consumer electronics device. The use of a wireless interface overcomes the problems associated with the distance between the first consumer electronics device and the second consumer electronics device, as well as the associated connector compatibility issues where the respective consumer electronics devices may not be equipped with compatible connectors or interfaces. Therefore, the present wireless interface for Removable Digital Content Security Devices adds a wireless interface to the Removable Digital Content Security Device so that content can be sent over a limited range transmission to other televisions or consumer electronics devices that may be located a short distance from the first television or consumer electronics device in order to enable the televisions and/or consumer devices to be easily relocated.

In operation, Applicants' system automatically discovers the presence of a second consumer electronics device that is capable of displaying the decrypted program content and is within wireless communication range of the removable security device that is connected to a first consumer electronics device. This second consumer electronics device is authenticated, and a link is established between the second electronics device and the security device that is connected to the first consumer electronics

device so that the decrypted content thereby can be shared among the multiple consumer electronics devices. The use of the wireless interface to serve multiple consumer electronics devices is not shown or suggested by the cited references, which are directed to the predetermined one-to-one linkage between a receiver/decoder to serve only a single associated display device.

This novel structure is now recited in Applicants' independent claims, such as claim 1, as follows:

> A wireless interface for Removable Digital Content Security Devices for delivering a stream of decrypted program content to a plurality of consumer electronics devices, comprising:
>
> security device means, removably connected to a first consumer electronics device, for receiving a stream of encrypted program content from a source;
>
> decryption means, located in said security device means, for converting said received encrypted program content to decrypted program content which is available to said first consumer electronics device;
>
> identification means, located in said security device means, for automatically discovering the presence of a second consumer electronic device not connected to said security device means or said first consumer device, which discovered second consumer electronic device is capable of receiving said decrypted program content;
>
> link management means for automatically establishing a wireless communication link from said security device means to said discovered second consumer electronic device;
>
> authentication means for authenticating said discovered second consumer electronic device; and
>
> wireless transmitter means for wirelessly transmitting said decrypted program content to said second consumer electronics device.

In contrast, the Gammie Patent discloses an embodiment of the prior art system referenced by Applicant in Figure 1, wherein a decoder is used to descramble encoded satellite transmissions. The decoder comprises an internal security module and a replaceable security module. The program signal is scrambled with a key, and then the key itself is twice-encrypted and multiplexed with the scrambled program signal. The key is first encrypted with a first secret serial number (SSN.sub.1) which is assigned to a given replaceable security module. The key is then encrypted with a second secret serial number (SSN.sub.2) which is assigned to a given decoder. The decoder performs a first key decryption

using the second secret serial number (SSN.sub.2) stored within the decoder. The partially decrypted key then is decrypted further by the replaceable security module using the first secret serial number (SSN.sub.1) stored within the replaceable security module. The decoder then descrambles the program using the twice-decrypted key. The replaceable security module can be replaced, allowing the security system to be upgraded or changed following a system breach. However, the security process described in the Gammie Patent is limited to the use of a decoder with a single associated television receiver. This security process is strictly a one-to-one communication exclusively between the decoder and the single associated television receiver. There is not even a hint in the Gammie Patent of the provision of the decoded program content to multiple devices, or the use of a wireless interface to automatically interconnect multiple devices which are capable of displaying the decoded content.

The Bilbrey Publication discloses a low-cost portable digital video player which receives proprietary compressed data from a personal video recorder (PVR) and displays the data on an integral display. Again, the low-cost portable digital video player described in the Bilbrey Publication is limited to the use of a low-cost portable digital video player with a single associated television receiver. This decompression process is strictly a one-to-one communication exclusively between the decoder and the single associated television receiver. There is not even a hint in the Bilbrey Publication of the provision of the decoded program content to multiple devices or the use of a wireless interface to interconnect multiple devices.

The Examiner also cites the well-known 802.11 protocol, where 802.11 wireless routers broadcast their SSID's and wireless enabled user devices discover the wireless networks; and if a user decides to connect to the router via wireless enabled user device, the router and wireless enabled user device set up a communication link. However, again, this is a one-to-one wireless connection, where the router transmits content to the attached user device. The router is not an end user device and does not make use of the data; it is simply a conduit for delivery of the data to the end user device. There is no hint of Applicants' Removable Digital Content Security Device which is removably installed in a first consumer electronics device and receives coded program content that is transmitted by a program source. The Removable Digital Content Security Device decodes the received content for use by the consumer in the first consumer electronics device. Applicants' Removable Digital Content Security

Device also includes a wireless interface which serves to deliver the decoded program content to a second consumer electronics device. There is no analogous structure in the 802.11 protocols where a user device forwards program content to another user device as is recited in Applicants' independent claim 1.

Applicants believe that the Examiner has not made a prima facie showing of obviousness for the claimed invention under 35 U.S.C. §103(a). The MPEP and courts have stated that the prior art relied upon by the Examiner must disclose all of the following:

> 1.) A motivation or suggestion to combine references; 2.) A reasonable expectation of success from combining the references; and 3.) The combined references teach all of the limitations of the claimed invention. MPEP §706.02(j); See also *In re Vaeck*, 20 USPQ2d 1438 (Fed. Cir. 1991).

If any of these requirements are not met, the combination of the references does not establish a prima facie showing of obviousness for the claimed invention. The Examiner has not met the requirements of item 3 of this test as noted above, since none of the cited references disclose Applicants' claimed automatic discovering of a second consumer electronics device, the provision of the decoded program content to both the first and second consumer electronic devices, and the use of a wireless interface to interconnect these devices:

> identification means, located in said security device means, for automatically discovering the presence of a second consumer electronic device not connected to said security device means or said first consumer device, which discovered second consumer electronic device is capable of receiving said decrypted program content;
>
> link management means for automatically establishing a wireless communication link from said security device means to said discovered second consumer electronic device;
>
> authentication means for authenticating said discovered second consumer electronic device; and
>
> wireless transmitter means for wirelessly transmitting said decrypted program content to said second consumer electronics device.

Therefore, since none of the references cited by the Examiner, individually or in combination, teach all of the limitations of the claimed invention, Applicants believe that independent claims 1 and 4 are allowable under 35 USC §103(a). In addition, Applicants believe that dependent

claims 2, 3, 5, and 6 are allowable under 35 USC §103(a), since these claims depend on allowable base claims.

In view of the above amendments and remarks, Applicants believe the pending application is in condition for allowance. Applicants believe no fee is due with this response. However, if a fee is due, please charge our Deposit Account No. 50-1848, under Order No. 013208.0133PTUS from which the undersigned is authorized to draw.

Respectfully submitted,
PATTON BOGGS LLP

Dated: August 11, 2008

By: /James M. Graziano/
James M. Graziano
Registration No.: 28,300
(303) 830-1776
(303) 894-9239 (Fax)
Attorney for Applicants

Customer No. 24283